

安全技术

基于双线性对的匿代理盲聚合签名方案

毛卫霞, 李志慧, 柳 焯

(陕西师范大学数学与信息科学学院, 西安 710062)

收稿日期 修回日期 网络版发布日期 接受日期

摘要 利用聚合签名的优点, 提出一种基于双线性对的匿代理盲聚合签名方案。聚合签名能将 个签名聚合成唯一的一个短签名, 从而使 个验证等式减少为一个验证等式。理论分析证明, 该方案保护了代理签名人的隐私权, 使签名的消息不可见, 在事后引起争议时还可以追踪到代理签名人的身份。

关键词 [代理签名](#); [匿签名](#); [盲签名](#); [聚合签名](#); [双线性对](#)

分类号 [TP309](#)

DOI:

通讯作者:

作者个人主页: 毛卫霞;李志慧;柳 焯

扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(73KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [参考文献\[PDF\]](#)
- ▶ [参考文献](#)

服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中 包含“代理签名; 匿签名; 盲签名; 聚合签名; 双线性对”的 相关文章](#)
- ▶ [本文作者相关文章](#)